ABSTRACT

Method and apparatus for handling calls from relocated instrumented functions to functions that expect a return pointer value in an original address space. In various embodiments of the invention, instrumented versions of selected functions of an executable program are generated and stored in a relocation address space. When a function is called by a function in the relocation address space, a return pointer register stores a first return-pointer value that is an address in the relocation address space. The address in the original address space that corresponds (logically) to the first return-pointer value is identified as an original return-pointer value. The first return-pointer value is associated with the original return-pointer value, references to the original return-pointer value are substituted for references to the first return-pointer value, and the instruction at the address indicated by the original return-pointer value is replaced with a breakpoint. When the breakpoint is encountered upon return of control at the original return-pointer value, the first return-pointer value that is associated with the original return-pointer value is obtained, and control is transferred to the instruction at the address referenced by the first return-pointer value.